REMARKS

Reconsideration and allowance are respectfully requested in light of the above amendments and the following remarks.

The Abstract has been amended to place it in compliance with U.S. practice. In addition, claims 1-5, 8-18, 21 and 22 have been amended to define the invention with additional clarity and to place all claim elements in non-means-plus-format. No new matter has been added.

With regard to art based rejections, claims 1-24 were rejected under 35 U.S.C.§102(e) as allegedly being anticipated by U.S. Patent Publication 2005/0010786 A1 to Michener et al. (hereinafter "Michener"). This ground of rejection is traversed.

The Office Action proposes that Michener discloses (1) generation of a key from another key and a unique identifier, (2) communication means for exchanging information between devices and (3) combining of the key and the unique identifier and storage of keys.

The Applicant notes that Michener discloses a Trusted Authorization Device (TAD) 10 connected to a client for authorization by a user 14 of a transaction downloaded by the client (1 or 2) to the TAD 10. Michener discloses that in order for a transaction to be authorized, the user 14 may couple a unique

security token 40 to a reader 22 of the TAD 10 and then enter a Personal Identification (PIN) Number. Once the user has authorized a transaction, the TAD 10 generates: a random number R; a second information responsive to a first information that incorporates the random number R and a first identification code; a digital signature of the second information; a set of transaction-specific session keys from a set of stored working keys using a 3-DES encryption process; a third information by encrypting the combination of the second information and its digital signature. Finally, a data structure comprising the plain text random number R, the plain text first identification code and the third information, is communicated to the client 12.

In addition, Michener also discloses at column 2, lines 19-24 that a key loading unit 38 and the TAD 10 can both independently use the key generating process 500 with a second identification code of the TAD (TADID_B) as a seed and a set of firmware keys can be used as the generating keys to generate a set of maintenance keys.

However, in Michener either the TAD 10 of the key loading unit 38 generates the base key from a master group key (the working key or firmware key) using a unique identifier (R or TADID_B) independently of any other device. There is no communication

between the devices during the key generation process.

By contrast, the present claimed invention provides a system that generates at least one unique base key, wherein at least two different devices (the cryptographic device and the security token), use a communication section to exchange data.

More particularly, the security token sends its unique identifier to the cryptographic device, so that the cryptographic device can generate the base key by combining its master group key with the unique identifier of the security token. The cryptographic device uses the communication section to send the generated base key to the security token which includes data storage section that stores the at least one generated unique base key.

Accordingly, the present claimed invention is distinguishable over Michener at least because Michener does not anticipate a data processing system having two different devices that each comprise a part of the information and/or have the capability to generate and store a base key.

Michener, by contrast, discloses that each of the described devices include all the elements to independently generate and store a base key.

In the present claimed invention, there is an advantage in

that as the security token does not know the master group key, it would be very difficult to breach the system, whereas in Michener it is possible to decipher the master group key.

For at least the above reasons, it is respectfully submitted that claim 1 is not anticipated by Michener, nor is the method of claim 5. The claims dependent from claims 1 or 5 are allowable at least for their dependence on an allowable base claim, and because of their recitation of an independent basis for patentability. For example, in claims 4 and 6, the unique identifier is not used as a seed, but rather is digested by the message digest function.

With regard to independent claim 9, it is respectfully submitted that Michener fails to disclose a system for performing symmetric keys based on mutual authentications between at least two security tokens.

Also, Michener fails to disclose a logic operator as claimed for processing the first base key and for the second unique identifier to produce a first composite key, or a second logic operator for processing the second base key and the first unique identifier to produce a first composite key.

Moreover, Michener does not disclose a message digest operation is operated on the unique identifier processed by the security token of the logic operator. Nor does Michener disclose

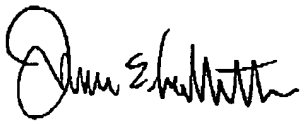
the use of random numbers used by a cryptographic section that encrypts the random numbers with composite group key to produce a cryptogram.

In view of the above, it is submitted that this application is in condition for allowance and a notice to that effect is respectfully solicited.

This amendment generates no new government fees.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,



Date: October 31, 2005

James E. Ledbetter
Registration No. 28,732

JEL/SG/att
ATTORNEY DOCKET NO. L741.02101
STEVENS, DAVIS, MILLER & MOSHER, L.L.P.
1615 L STREET, NW, Suite 850
P.O. Box 34387
WASHINGTON, DC 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200

Abstract of the Disclosure

A data processing system and method for performing mutual authentications between two security tokens by generation of a common cryptographic key, wherein the common cryptographic key is generated using unique identifiers associated with each security token that diversify a common master key. The generation process incorporates a message digest function such as SHA-1 and an XOR operator to arrive at the common symmetric key.